GUIDE TO THE SARBANES-OXLEY ACT: MANAGING APPLICATION RISKS AND CONTROLS

Frequently Asked Questions

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

Introduction

Since the passage of the Sarbanes-Oxley Act ("SOA" or "Sarbanes-Oxley"), Protiviti published several editions of frequently asked questions addressing many topics pertaining to compliance with various provisions of the Act, and in particular with Section 404. For example, our Third Edition of *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*, our *Guide to the Sarbanes-Oxley Act: IT Risks and Controls* and other knowledge publications are freely available for download at **www.protiviti.com**. They serve as companion documents on internal control reporting requirements.

We are publishing the *Guide to the Sarbanes-Oxley Act: Managing Application Risks and Controls* with the intention of building off of our prior publications by providing more specific guidance on how to identify relevant applications and the related risks that are important to SOA compliance, and how to most effectively test the controls that mitigate these risks. The questions listed in this document are ones that have arisen in our discussions with clients and others in the marketplace who frequently deal with SOA compliance matters and are focused on improving internal control over their critical business applications. While the broader context is organizations' efforts to address Sarbanes-Oxley, the questions we address herein are relevant to anyone interested in improving and relying on their applications' data integrity, regardless of their compliance initiatives. The document also contains numerous references and examples related to market-leading Enterprise Resource Planning (ERP) applications. It is important to note, however, that the concepts presented here apply to more than ERP systems. They are relevant to all types of applications, including in-house development, second-tier applications, best-of-breed solutions, industry-specific packages, Web-enabled tools, etc. Examples of areas that are discussed within this publication include suggestions for effectively segregating incompatible duties, efficiently testing complex application security, and utilizing automated application controls to reduce the burden of tedious manual procedures. The responses and points of view expressed herein are based on Protiviti's experience assisting companies as they document, evaluate and improve their internal control over financial reporting.

As many companies complete their second year of Sarbanes-Oxley compliance, executives and audit committees are expecting more value with lower costs. Fulfilling these expectations will require a shift from simply repeating the same SOA project each year to a sustainable, cost-effective compliance process that is embedded into business as usual. For many companies, we strongly believe that significant opportunities to improve the efficiency and effectiveness of their SOA compliance efforts reside at the application level. We also believe that optimizing and further leveraging the capability of applications can increase business-process cost-effectiveness, enhance a company's control environment and reduce compliance costs. These results lead to an increased Return on Investment (ROI) for the financial and human resources spent on the application and compliance investments.

The focus of Protiviti's Application Control Effectiveness (ACE) team is driven by a commitment to a sustainable, cost-effective and value-added process. Our ACE team possesses deep competencies and experience as they relate to applications, technology risk, internal audit, internal controls, business processes and SOA compliance requirements. We leverage this diverse expertise and our automated assessment tools for our clients to assist them in optimizing their applications to derive value-add from their Sarbanes-Oxley compliance efforts, including stronger internal control environments and more cost-effective business processes.

While we expect that readers will find the guidance herein to be valuable and thought provoking, this publication is not intended to be a legal analysis in terms of the suitability of approaches in complying with the requirements of Sarbanes-Oxley and other legal requirements. Companies should seek legal counsel and appropriate risk advisors for answers to specific questions as they relate to their unique circumstances. Company approaches may be impacted by changing standards, and evolving technology and application functionality.

Protiviti Inc.

May 2006

Section 1: Looking Forward

During the first two years of SOA compliance, most companies relied on manual controls for a variety of reasons. One of the prime reasons in the first year was the lack of early guidance on exactly how to achieve compliance and the resulting time pressures to "just get it done." The second year was not much different from the first because most companies didn't have enough time to plan for control improvements. However, compliance requirements are ongoing and require a sustainable compliance ***process***, as opposed to an annual compliance ***project*** dependent upon the heroic efforts of a few individuals.

Sustaining the level of effort required to operate, maintain and document manual controls is significant. Leveraging ERP functionality and embedded controls is an opportunity to turn the "compliance burden" into value-add by optimizing the use of the organization's ERP and increase ROI by moving from a compliance project to a compliance process. In addition, there are opportunities to reduce the amount of compliance testing by testing one automated control to establish that there is a preventive mechanism in place that disallows an event to occur as opposed to performing multiple tests of manual controls to demonstrate that an event has not occurred even though it is permitted. Achieving these improvements accomplishes significant reduction in risk and shifts the organization towards optimization of the control environment. Figure 1 shows how this evolution may occur.

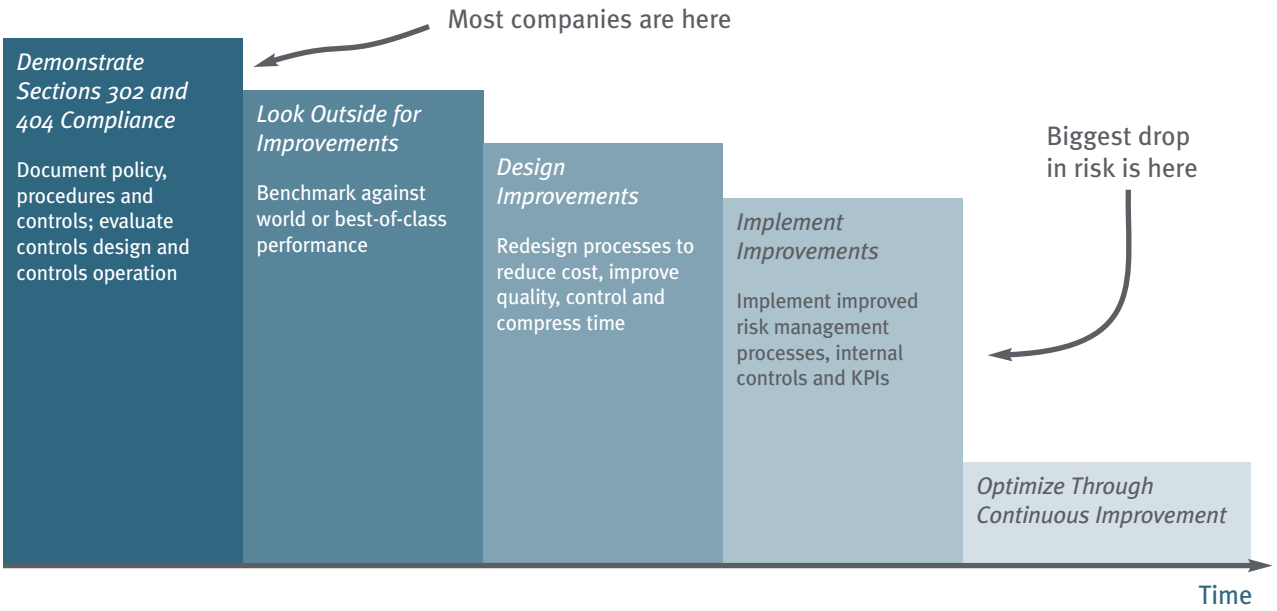

Figure 1

We believe that many organizations will be actively working over the next 12 to 18 months to identify ways to reduce their overall compliance costs while achieving improvements to their risk management structure. The "project to process" transition to improve the quality and sustainability of the internal control structure and make the compliance process more value-added and cost-effective will take some time. It is a journey to a better place than what we see in the current environment in which many interested parties are expressing concern over the high cost of compliance. Those organizations that accomplish the "project to process" transition to improve quality, time and cost performance while simultaneously reducing financial reporting risk will be able to secure a stronger competitive position in the marketplace. The differentiating advantage of a strong reputation will sustain investor confidence and command higher multiples over time. Similarly, those organizations that lag behind in this transition will continue to incur higher compliance costs and face increased financial reporting risk to their organization, leading to less investor confidence and lower multiples over time.

Section 2: General Application Risk and Control Considerations for Complying with Sarbanes-Oxley

1. What does SOA Section 404 say about an organization's reliance on critical business applications?

Section 404 of the Sarbanes-Oxley Act does not address ERP systems and other applications specifically; however, the SEC and Public Company Accounting Oversight Board (PCAOB) have addressed this topic in their releases and standards pertaining to Section 404 of the Sarbanes-Oxley Act.

According to the SEC Staff's Statement on Management's Report on Internal Control Over Financial Reporting, May 16, 2005, management cannot defer its obligations, as defined by Section 404, just because a new application or information system is implemented in the current fiscal year. The SEC also emphasized that companies are required to prepare reliable financial statements following the implementation of new information systems. In that sense, the goals of Section 404 align with management's existing responsibilities when undertaking an IT conversion or implementation project. Specifically, the SEC staff noted "with respect to system changes, management can plan, design, and perform preliminary assessments of internal controls in advance of system implementations or upgrades." The staff went on to say that "…not all testing must occur at year-end. As a result, the staff does not believe it is appropriate to provide an exclusion by management of new IT systems and upgrades from the scope of its assessment of internal control over financial reporting."[1]

In the Questions and Answers published by the PCAOB Staff on May 16, 2005, the PCAOB staff clarified for auditors the level and extent of testing that is required with respect to automated application controls and reinforced the concept of benchmarking application controls. Specifically, in Question 45 the PCAOB staff noted:

> Entirely automated application controls, therefore, are generally not subject to breakdowns due to human failure and this feature allows the auditor to "benchmark," or "baseline," these controls. If general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor last tested the application control, the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests of the operation of the automated application control. ... the nature and extent of the evidence that the auditor should obtain to verify that the control has not changed may vary depending on the circumstances, including depending on the strength of the company's program change controls.[2]

Finally, with respect to determining the appropriateness of a benchmarking strategy, the PCAOB staff stated:

To determine whether to use a benchmarking strategy, the auditor should evaluate the following factors:

- The extent to which the application control can be matched to a defined program within an application;
- The extent to which the application is stable (i.e., there are few changes from period to period); and
- Whether a report of the compilation dates of all programs placed in production is available and is reliable. (This information may be used as evidence that controls within the program have not changed.)

To determine whether to reestablish a benchmark, the auditor should evaluate the following factors:

- The effectiveness of the IT control environment, including controls over applications and systems, software acquisition and maintenance, access controls and computer operations;

---

[1] *SEC Staff Statement on Management's Report on Internal Control Over Financial Reporting*, May 16, 2005

[2] *Questions and Answers published by the PCAOB Staff on May 16, 2005*

- The auditor's understanding of the effects of changes, if any, on the specific programs that contain the controls;
- The nature and timing of other related tests; and
- The consequences of errors associated with the application control that was benchmarked.[3]

In summary, the guidance and clarification by the SEC and PCAOB underscore the following critical points:

- System-based controls (e.g., application configurable controls) are more reliable than manual controls.
- Application configurable controls can be "baselined" or confirmed to be operating effectively once and then the focus of testing can move to the validation of general computer controls, including change control procedures and security administration, and any newly implemented controls subsequent to the testing of the established baseline.
- Once application configurable controls are "baselined," it is not necessary to test the same controls each successive year.
- Significant annual efficiencies can be achieved in the testing of application configurable controls if existing general computer controls, including change control and security administration, are operating effectively.
- Significant annual efficiencies can be achieved by continuing to increase the number of configurable controls that are relied upon relative to manual controls.
- It is far more efficient and effective to proactively design controls into an application than to inspect and audit them post-implementation.

It is clear from the SEC and PCAOB releases and standards that system-based controls play a vital role to the sustainability of effective internal control over financial reporting. In fact, the PCAOB included examples in Appendix B to Auditing Standard No. 2 that illustrate the importance of integrating system-based controls into the assessment of internal control over financial reporting.

2. What is a public company required to disclose regarding an ERP/application implementation?

We have noted an increase in the amount of information provided in disclosures relating to ERP implementations, both in company 10-Ks and 10-Qs. Many companies also have identified the implementation of an ERP as a significant change in internal controls, as defined by Sarbanes-Oxley and the SEC's rules and regulations, as process reengineering and related changes to the control environment generally accompany a major ERP implementation.

In many cases, the content of quarterly company disclosures leading to and at the go-live point generally have contained references to (a) previously reported Sarbanes-Oxley Section 404 results and (b) the efforts undertaken to ensure that the impact on the control environment was appropriately considered in the design and implementation of the ERP. The intent is often to maintain, with emphasis on enhancing, the system of internal control over financial reporting. Sarbanes-Oxley requirements do not specifically oblige a company to conclude upon the design effectiveness and operating effectiveness of the control environment at the time of the implementation. However, management is required to do so as of the end of the company's fiscal year. In addition, companies are expected to disclose significant improvements to internal controls. This point is discussed further in Question 170 of the third edition of Protiviti's *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements.*

[3] *Questions and Answers published by the PCAOB Staff on May 16, 2005*

When implementing a new application critical to financial reporting, we strongly recommend several key steps:

1. The company should establish a control baseline upon go-live, as described in our response to Question 7, and integrate the requirements of Sarbanes-Oxley into the functional design specifications and the related testing of the solution.

2. An organization implementing a significant application should perform a control design assessment during the overall design of the solution and update the related Sarbanes-Oxley compliance documentation (e.g., process flows, process narratives, risk-control matrices, etc.) as necessary.

3. Process owners and participants should understand the controls they are expected to perform as part of their utilization of the new application. Therefore, user training is a critical element to ensuring an effective control environment as it relates to the utilization of any application, particularly an ERP.

4. Finally, an organization implementing an ERP/major application should involve its external auditors in the planning process and obtain guidance from its auditors on design and disclosure requirements. Advice from legal counsel also should be sought on the appropriate disclosures.

These proactive steps will help facilitate an efficient and effective overall Sarbanes-Oxley compliance effort for the fiscal year and reduce the risk of costly surprises at fiscal year-end.

The following is an example of a disclosure in a filing to the SEC relating to an implementation of an ERP:

> The company is in the process of implementing an ERP system in all of its businesses to support the company's growth plan. The phased implementation is currently planned to be complete by 2006. Implementing an ERP system on a widespread basis involves significant changes in business processes and extensive organizational training. The company currently believes a phased-in approach reduces the risks associated with making these changes. (The Company) believes it is taking the necessary steps to monitor and maintain appropriate internal controls during this transition period. These steps include deploying resources to mitigate internal control risks and performing additional verifications and testing to ensure data integrity. The company has undertaken a comprehensive review of the effectiveness of its internal control over financial reporting as part of the reporting, certification and attestation requirements of Section 404 of the U.S. Sarbanes-Oxley Act of 2002. For the year ended December 31, 2004, the company's internal controls were found to be operating free of any material weaknesses. In connection with the continued implementation of its ERP system, the company expects there will be a significant redesign of its business processes during 2005, some of which relate to internal control over financial reporting and disclosure controls and procedures.

3. What are the typical application control types as they relate to SOA Section 404 compliance?

COSO defines application controls as, "Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing." There are six primary areas of application controls which should be considered with respect to Section 404 compliance:

1. ***Automated process controls:*** Automated process controls are those controls addressed by application functionality. These controls can be codified controls that an application enforces based on programmed code and typically require application developers or programmers to modify or maintain. For example, most applications will not allow an unbalanced journal entry to post. For organizations with in-house developed applications, many of the controls require IT developers to maintain them. However, for organizations with applications, many automated process controls can be configured to operate according to the organization's specific policies, rules and strategies. Configurable controls are "switches" that can be set in an application by turning them on or off to secure data against inappropriate processing. Configurable controls include posting limits, release strategies, tolerances, validations and edits, screen layout, authorization groups, transaction variants, exception reports and security settings. Configurable controls can be either preventive or detective in nature. Examples of configurable controls include tolerance limits with respect to purchase orders and invoice variances,

acceptable ranges for determination of useful lives for asset classes or required fields for posting manual journal entries. Within each critical business process or transaction cycle, configurable controls addressing critical process risks should be identified and relied upon as appropriate. Where feasible, organizations should seek to continually optimize the use of and reliance upon configurable controls to both improve the sustainability and cost-effectiveness of the control environment and increase the efficiency of the testing of critical controls. For more on these controls, see Section 3.

2. ***Manual process controls that may be candidates for automation:*** No matter how integrated an application may be, generally an organization employs critical manual controls that operate outside of the application to ensure the integrity of the data and reliability of financial reporting. Examples of manual controls include account reconciliations and approvals. An organization should consider all possible opportunities to "convert" manual controls to system-based controls, where feasible, in order to increase the effectiveness of the control as well as the efficiency by which the control can be validated.

3. ***Interface/integration controls:*** An SOA compliance approach should ensure interfaces between applications are considered as risk factors in the financial reporting process, particularly if the interface is manual (e.g., download of data from one application for upload/entry to another). Controls that ensure the data integrity of the interface should be identified and validated. Organizations should document and assess how files are transferred, how users assure business transactions are authorized before being transferred, and whether any reconciliation procedures or other tools help ensure completeness and accuracy of the interface. For example, if an organization utilizes a payroll application which interfaces with the core financial reporting application, the controls addressing the inherent risks relating to the "hand-off" of critical data between the two applications should be identified and validated. It is just as important to evaluate these controls as it is to assess the critical controls within each individual application. For more on these controls, see Question 34.

4. ***Reporting controls:*** Reporting controls are necessary to ensure reports generated from the application accurately reflect the financial position of the organization. The compliance team should assess risk from the financial reports back to the source system to ensure all risks and controls are considered within and outside the application. This includes consideration of report design and maintenance processes as well as processing governing the manipulation of extracted data outside the application. A common example is an organization's download of financial data from the core financial reporting application (e.g., an ERP) into a spreadsheet for use in preparing financial reports and disclosures, including EDGAR formats for filing with the SEC. Controls should be identified and validated that address the risk of the data being modified inappropriately subsequent to the download of the data and prior to the final preparation of the financial statements. All of the aforementioned configurable, application and interface controls are rendered useless if a risk at this point in the financial reporting process remains unmitigated.

5. ***Application security, particularly as it relates to segregation of duties (SoD) and access to sensitive transactions:*** Different from security administration, this area relates to the risks that individuals or groups have been granted inappropriate or excessive access to an application, resulting in the ability to perform conflicting duties (e.g., set up a vendor/pay a vendor) and/or inappropriate/unnecessary access to sensitive transactions (e.g., vendor pay data or ability to modify critical application configurations). Application security should be considered for each critical business cycle to ensure appropriate access based upon a succinct role definition. The access defined for each role should be free of any conflicting duties. From there, roles should be allocated to individuals who perform the specific roles defined. Care should be taken to ensure that no individual is assigned a combination of incompatible roles that create a conflict. For more on these controls, see Section 4 below.

6. ***General computing controls (GCC) that impact the application, including change control, security administration and computer operations:*** These controls are critical, as they address the risks of inaccurate and/or unauthorized changes, access to the application, the related database and network, and the maintenance of the general IT environment that could impact the integrity of the data produced by the application. For more on these controls, see Section 5.

4. Why is it so important to consider embedded system-based (e.g., ERP) controls for financial reporting and Sarbanes-Oxley compliance?

Generally speaking, system-based controls are more reliable and sustainable because they are not as susceptible to human error or breakdowns as are people-based controls. These controls are also more cost-effective to test than manual-based controls, so long as they are designed, maintained and secured effectively. When evaluating the appropriate mix of system-based and people-based controls, there are two fundamental points to keep in mind. First, data integrity is essential to the production of accurate financial reports. Second, the controls within the application and access security configuration of an application are critical to ensuring data integrity. For example, if the application is not configured to ensure that a posted manual journal entry is balanced (e.g., debits equal credits), the reliability of financial reports could be impacted.

Many organizations have implemented applications such as SAP, Oracle, PeopleSoft, JD Edwards, Lawson, etc. These applications provide multiple benefits including improved integration and standardization across the business and an increased ability to customize business processes through configuration. It is important to note that, due to the integrated nature of ERP systems, the vast majority of transactions ultimately impact financial reporting. Therefore, everyone who has access to the ERP, from the shop floor to the accounting department to the executive suite, can impact the reliability of financial reporting. For example, if established security roles allow an individual to both propose and post a journal entry without any approval, a segregation of duties conflict would arise and expose the organization to possible errors and omissions in financial reports.

5. How should the Section 404 compliance team determine the critical applications for each key business process?

After high-priority financial reporting elements and related high-priority processes are identified, a critical part of the compliance effort is identifying the applications that are utilized in the high-priority processes. These applications are likely to impact the priority financial reporting elements. In analyzing any critical business process, the compliance team should document the key inputs, processing activities and process outputs. This documentation should include a description or map of the application systems that are an integral part of the process. For more on documentation, see Section 7.

The related critical applications for each significant business process that are involved in the data flow from the originating transaction to financial statement generation (including all access points into applications and hand-offs and interfaces between applications) should be identified and prioritized. In other words, the compliance team should select the applications that (a) are integral to the success of the process in achieving its objectives, and/or (b) expose the process to increased risk of not achieving relevant financial reporting assertions. These applications should be integrated into the documentation and evaluation process.

Some factors to consider when prioritizing applications include:

- The volume of transactions processed (typically, the higher the volume, the more critical the application)
- The dollar amount of the transactions (typically, the larger, the more critical the application)
- The complexity of the calculations – complex in this situation means the ability of the users to determine the propriety of the calculation (typically, the more complex, the more critical the application)
- The sensitivity of the data and transactions (typically, the more sensitive, the more critical the application)

The importance of proper application identification is illustrated in the following chart:

BUSINESS PROCESS	APPLICATIONS				
	ERP	Consolidation	HR	Supply Chain	Other
General Ledger Accounting	●	●	●	●	
Purchase Materials and Supplies	●			●	
Process Payroll and Benefits	●		●		
Process Accounts Receivables	●			●	
Manage Inventories	●			●	
Other Business Processes	●				●

Many companies employ an ERP solution (e.g., SAP, Oracle) for their general ledger, but complement that solution with a financial consolidation solution (e.g., Hyperion) for financial reporting purposes. As many companies began Section 404 compliance activities, they realized that their ERP access structures gave users excessive authorizations and data access. In response, these companies re-implemented authorization and data access structures within the application to ensure proper restrictions. However, users could still freely access equivalent data via the consolidation application, thereby circumventing the intended security restrictions. Thus, without also identifying the consolidation application as a critical element within the security assessment scope in addition to ERP security, this organization's assessment would be insufficient. When the applications are being identified and prioritized, it is important to identify ALL applications used, including worksheets, spreadsheet macros, user-database programs (e.g., Microsoft Access), and Web-based programs and calculators.

In summary, it is important to identify the complete universe of applications utilized within the organization that enable critical processes to perform and produce key financial statement elements. This effort will enable the compliance team to determine which key applications fall within the compliance scope and ensure that the Section 404 documentation and control assessment is complete.

6. Should the evaluation of application controls be integrated within business processes or performed separately?

Application-specific controls are a critical part of business processes and ideally should be documented and evaluated simultaneously alongside the manual business process controls. The compliance team needs to consider the process risks and key control points, and determine which controls are programmed application controls (such as an automated three-way match) and which controls rely upon computer-generated information to operate effectively (such as an exception report). Manual and application-related controls do not operate in a vacuum. They are oftentimes not mutually exclusive. Therefore, it is important to identify and assess them together in order to identify control dependencies and achieve a holistic assessment of the business process as a whole. The PCAOB included case examples in an appendix to Auditing Standard No. 2 that illustrate this point.

By considering manual and related application controls simultaneously within a business process, the compliance team will be far more likely to identify a more sustainable and efficient mix of manual and application controls in terms of testing controls operating effectiveness. In addition, the compliance team also will be able to identify opportunities to further automate manual controls.

Once the key application and manual controls are identified for purposes of Section 404 compliance, the team then needs to consider the necessary steps to fully understand and document those controls within the application. Skills and resources are important factors to consider when planning these steps (i.e., the necessity to use a specialist to understand the design and operations of critical application systems and the control capabilities embedded within those systems).

7. How is an appropriate application baseline established?

Key elements of establishing a baseline for a given application include:

- ***Establish baseline scope:*** Identify key application controls, programmed functions and reports that are relied upon to help assure complete, accurate, timely and proper processing and reporting of transactions. The identified population of controls, functions and reports creates the baselining scope.
- ***Document configurable controls and supporting general application processes:*** Document configuration settings and business rules for the controls, functions and reports, and obtain approval by appropriate management that such settings and rules are expected within the application (e.g., ERP).
- ***Establish/validate processes and controls relative to security administration and change management:*** Document and validate the administration and maintenance of access security specific to the application. In addition, document and validate change management relative to the application's core logic.
- ***Validate operation of configurable controls and general application processes:*** Validate that the established baselines are operating and utilized as designed and documented. This can be achieved through:
  - Review of existing application implementation documentation, including unit/integration testing, system testing, and/or user testing and business sign-off.
  - Reperform the control or function through automated or manual testing. For example, use available automated testing tools to provide evidence of existing configurations and validation of change control procedures. See Sections 8 and 10 for further discussion of testing techniques and automated testing tools.
- ***Baseline maintenance and change management:*** Maintain the baseline verification documentation, ensure and validate consistent performance of general application controls (e.g., change management and security administration) and document and test any changes to either the application or the general IT control environment.

For those organizations with multiple critical applications (e.g., more than one ERP) and/or multiple instances and installations of a given application, standardization of the organization's change management and security administration processes across all applications can improve the control environment. It also can achieve significant efficiencies in the assessment of the applications that have been baselined, as described above.

8. Is it possible to rely solely on manual controls, negating the need to consider and evaluate application controls?

Perhaps, but we strongly advise companies not to do this. Not only are manual controls difficult to operate in a sustainable fashion, these activities by nature are more susceptible to control failure due to human error and inconsistent attention. In addition, it is extremely expensive and inefficient to maintain, test and rely primarily or solely upon manual controls, effectively negating management's investment in IT applications.

Audit committees and senior executives are driving compliance officers to reduce the expense of operating and assessing financial reporting controls while simultaneously increasing their effectiveness. An essential step in the Sarbanes-Oxley compliance journey is in the transition from an ad hoc project, which most organizations experienced in the first two years, to a sustainable, cost-effective and value-added process over time that includes an increased reliance on automated controls.

The concept is not new. The reengineering trend of the 1990s focused on enabling functionality, giving rise to the prevalence of integrated ERP systems such as SAP, Oracle, PeopleSoft, JD Edwards and others. Although these applications mechanized many operational and financial transactions, the automation of *internal controls* continued to be a stretch goal that many organizations failed to achieve. This was partly due to the point of view that controls were often "in the way" of a company's reengineering efforts. In addition, many companies assumed that since they were using an "off the shelf" ERP system, they were benefiting from all the necessary system controls provided by that system. However, controls were not typically the primary focus or functional strength of the ERP implementation team.

Today is a new era. Sarbanes-Oxley and other governance requirements have established unprecedented pressure to enable timely and reliable financial reports and enforce positive control assertions every quarter. The controls that support achievement of these objectives must be precisely executed and fully confirmed every year. Initially, many companies overwhelmingly relied on manual controls and adopted traditional but tedious "block-vouch" type testing. Unless the controls portfolio is reevaluated with an eye towards striking an optimal balance of automated and manual coverage, these companies will be stuck repeating the same painful, expensive approach every year.

9. What are the benefits of control automation?

Control automation can provide significant benefits to most organizations. Some examples of these benefits include:

- **Decrease in employee time** conducting or supervising tedious manual controls;
- **Decrease in the cost of annual assessments** through replacing slow, manual, error-ripe testing with the far more efficient observation of an online setting;
- **Reduction in the odds of human error and fraudulent manipulation** through forced online consistency and compliance;
- **Increase in quality and reduction in rework** by detecting problems more quickly and placing emphasis on preventing them altogether; and
- **Proactive management of audit fees** by applying the same logic of test savings to external audits and achieving increased auditor reliance on internal testing of safer automated controls.

There may be resistance to change from tired compliance teams that are just getting comfortable with the existing internal control structure. However, the opportunity for long-term savings is too great to ignore, not to mention the need to respond to increasing pressure from external auditors to rely more on automated controls. Therefore, a fresh study of automation opportunities should be carefully considered to maximize ongoing value and avoid competing against companies with a lower cost structure. Failure to automate in high-value areas may institutionalize a high-cost internal control structure built on excessive reliance on inefficient manual controls.

10. What factors should an organization consider when determining which manual controls to automate?

To move a control structure and the associated testing toward reliance on automated controls takes time. It will require input from a variety of internal business constituents and at least some technology investments. In this regard, organizations should begin by examining the sources of evidence supporting management's conclusion as to the operating effectiveness of internal control over financial reporting. This examination ordinarily should drive efforts to start rebalancing the automated controls portfolio.

The effort begins with a fresh look at the organization's current key controls, with an eye towards several factors. We have found controls automation efforts to be most successful in yielding value-added benefits when they are:

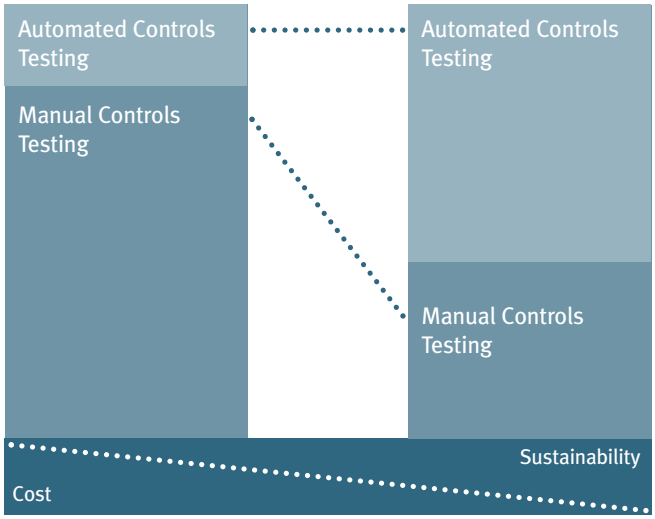

Figure 2

- Applied through an integrated solution (e.g., ERP), because the improvements have a multiplier effect across common processes;
- Used to replace manual controls that are particularly expensive to operate and test;
- Utilized in risk areas that have the most impact on reports and performance if controls fail;
- Employed in areas of heightened external audit sensitivity, such as segregation of duties, an area of concern to the audit firms;
- Directed toward current practices that are more prone to error and breakdowns; and
- Operated in association with procedures that are repetitive and require little judgment or human intervention.

Applying the factors above to manual or poorly automated controls can help prioritize management's options for automating or optimizing controls.

Prerequisites to relying on automated controls include sound program and configuration change management controls as well as strong security controls. If either of these general controls is weak, automated controls are vulnerable to override by management and other personnel. In addition, the compliance team would be unable to prove conclusively that the automated controls remained intact through year-end.

A wealth of software packages exists to enable automation initiatives (see Section 10 for further discussion). However, it should be noted that automation is not appropriate for all situations. As always, there should be an evaluation of the holistic cost of change against the value of future savings and increased quality and effectiveness of the internal control structure.

11. How can an organization decrease its reliance on spreadsheets?

Many organizations have opportunities to better utilize the existing reporting capabilities of their applications. Often, when company representatives rely on reports or data generated from software other than their existing applications, it is a good indication that the individuals who utilize that software to support financial reporting aren't maximizing the reporting capabilities of their applications. Reliance on spreadsheets is a good example of this problem.

For example, many organizations often extract data from an application and download it to a spreadsheet application for custom sorting and filtering. This process may be undertaken without understanding that the application has similar capabilities built into its reporting functionality. Ultimately, this activity may be a result of inadequate user requirements analysis during implementation. Alternatively, it may be a training issue where the end users are not made aware of the functionality offered by the application. If this situation is prevalent throughout the company, management should consider it a possible risk. As individuals involved in the compliance efforts begin to fully understand the capabilities of their company's applications, they more fully realize the importance of using the reports generated from that application, as well as the control implications and related compliance costs and risks of not doing so.

Section 3: Application Control Considerations

12. What are configurable controls?

Application-specific control considerations relate primarily to the controls programmed within an application. These so-called "programmed controls" may be relied upon to mitigate business process level risks. In Question 4, "automated process controls" were introduced. Configurable controls are a subset of automated process controls.

Examples of configurable controls include tolerance limits and ranges, data integrity checks, data field requirements, workflow approvals, etc., which are implemented as part of an application solution. These controls facilitate complete, accurate and timely processing and reporting of transactions by financial reporting applications in accordance with management's prescribed criteria. These control considerations arise around critical business process flow points at which the application:

- Makes calculations
- Performs data validation and edit checks
- Interfaces electronically with other systems
- Sorts, summarizes and reports critical financial information that is relied upon as complete and accurate by management
- Limits access to transactions and data

The above application-level control considerations arise around the need to ensure the proper design of application controls and the fact that they operate as and when intended by management. These considerations are also based upon the presumption that neither the programmed controls are changed nor the application around the programmed controls is changed, such that the controls no longer perform as or when intended by management. As noted in Question 7, the organization should seek to "baseline" the critical configurable controls by initially establishing their operating effectiveness and then by validating critical general computing controls, including change controls and security administration processes. The established baseline then can be updated for any changes in configurable controls going forward.

Another term that is frequently utilized to refer to application-level controls is "inherent controls." Although this term is subject to interpretation, its most common use is in referring to data integrity controls that are "hard-coded" into an application. For example, the data flow of sales transactions in an ERP could result in data being "rolled up" from a sales order to manufacturing, to shipping, to inventory relief, to revenue recognition and recording, to accounts receivable and to the payment application. In effect, an organization is relying upon the inherent programmed control that this data transfer occurs accurately and timely. To differentiate between an inherent control and a configurable control, a configurable control in this situation would include an optional setting for approving price ranges used on sales orders based upon the product being sold, with the objective of reducing the risk of inappropriate prices or unacceptable price concessions. Another example of a configurable

control is a setting that would allow application of cash only if the amount is within a certain tolerance limit in relation to the stated invoice amount. Therefore, configurable controls are intended to be optional settings, whereas inherent controls are not. Modification to inherent controls generally requires modifying the application's core logic. Such modifications, if any, should follow the organization's change control process and related controls.

Sections 8 and 10 discuss testing of application controls.

13. How are key application controls identified for documentation and testing?

As with all major transaction cycles, it is critical to identify, prioritize and document the following:

- The major subprocesses and related applications within the overall process
- The transactions relating to each of the identified subprocesses, including major inputs, processing activities and outputs driving the transactions, and the related applications
- The risks and controls within each of those subprocesses

As noted in Question 6, it is critical to identify and consider application-related risks and controls simultaneously with other business process risks and controls arising from manual activities. This integration is important because it ensures an appropriate understanding of the interrelationship between manual controls and application controls. It also ensures a cost-effective and holistic prioritization and assessment of the risks and controls within the business process.

As it relates to the applications utilized within critical processes, and as discussed further in Section 2, it is critical to identify:

- Transactions and access rights deemed sensitive (e.g., the ability to process payments) within the application.
- The users who utilize the application to perform their individual job functions.
- Key segregation of duties conflicts that should be avoided within the process and the security administration process to maintain the desired security environment.
- How master data for the process is created, maintained and controlled within the application and the related change management process for that data.
- Critical inherent and configurable controls relevant to the process, including transaction data integration, general ledger and sub-ledger integration, tolerance limits, required fields, workflow approval, and warning and error messages.

A detailed understanding of application functionality relating to each major business process is the first step in successfully understanding the risk and control implications within the process. In this section, we specifically consider the functionality of ERP systems across major business cycles. While the basic process flow for each cycle noted below is similar across different ERP systems, each application has its own nuances that require a detailed knowledge of both the business process and the ERP itself to effectively assess the risks and controls within the process. Each of the major cycles addressed in this section can be configured to varying degrees in most applications. The system integration and functional design that is inherent in most ERP systems significantly expands the pervasiveness of the impact arising from poor system-based controls. Therefore, it is critical to ensure that configurable controls within an application are appropriately designed, implemented, maintained and secured.

The following questions give examples of critical control considerations, in addition to those noted above. The questions relate to the major business cycles of Order to Cash (Question 14), Procure to Pay (Question 15) and Close the Books/Financial Reporting (Question 16). We also have provided a few related examples of configurable controls specific to ERP systems such as SAP, Oracle, PeopleSoft and JD Edwards. The examples

below are not intended to be a complete listing of all configurable control possibilities pertaining to each of these applications. Our intent is to provide examples of configurable controls within the context of the major business transaction cycles and examples of the related functionality within a few applications.

14. What are some application control considerations for the Order to Cash cycle?

The Order to Cash (OTC) cycle in an ERP system encompasses all activities related to the sale, delivery, and billing of materials and/or services to the organization's customers. Activities within the ERP that support this major cycle include:

- Customer Master Data Maintenance
- Inquiries, Quotations, Pricing and Contract Administration
- Sales Order Processing and Credit Management
- Goods/Services Issue and Shipping/Delivery Processing
- Returned Material Processing
- Billing, Invoicing and Payment Processing
- Sub and General Ledger Updates

Throughout these processes there are several configurable controls and functions that should be considered. Examples include customer master record maintenance, duplication checks, pricing tolerances, invoice posting tolerances, duplicate invoice checks, dunning process, credit limits, credit memo limits, shipping-to-sales order tolerances, journal entry processing, transaction account impact and reconciliation, and revenue recognition and account determination.

The following illustrations expound on two of these controls:

- ***Customer Master Record Maintenance:*** SAP provides three controls that enable companies to prevent or discover duplicate customer master records. The first control provides search criteria for duplicate customers. SAP is preconfigured "out of the box" to search for duplicate customers based on customer name and address. However, this control only searches for duplicates and does not notify the person entering the data that there is a possible duplicate record; therefore, the control does not actually prevent duplication. The second control is also a configurable control that notifies the user with a warning or error message that there is a possible duplicate record based on defined search criteria. This second control is not typically enabled in SAP "out of the box" and must be "turned on" to deploy the search criteria. The final control is detective in nature and is a report typically delivered in SAP "out of the box." The report RFDKVZ00 facilitates the review of customer data for duplicates by listing all customers.
- ***Billing, Invoicing and Payment Journal Entry Processing:*** Similarly, the risk of invalid, incomplete, inaccurate or untimely changes to accounts may be addressed with security and process controls in an Oracle application environment by establishing security controls, such as:

  - "Cross-Validate Segments" in Key Flexfields – This setting restricts certain account code combinations from being created during journal entry processing.
  - Rules to control the extent of user access across Flexfield segment values and/or organization definitions.

  In addition to security controls, business process controls may be established. Such controls include the following:

  - Set-of-Books to "Require Journal Approval" – This setting enables journal entries to be approved based on preset authorization limits.

- Profile Option "Journals: Find Approver Method" – This setting routes the journal batch for approval to the appropriate individual.
- "Recurring Journals" – This setting provides for consistent booking of routine journal entries.
- "Journal Reversal Criteria" – This setting defines the reversal method, including period and date, so that reversal journal entries can be created and posted automatically.
- "AutoPost Criteria Sets" – This setting allows the selection and posting of journal entries based on defined criteria.
- "Elimination Sets" – This setting consistently eliminates general ledger balances in consolidation.

15. What are some application control considerations for the Procure to Pay cycle?

The Procure to Pay (PTP) process in an ERP encompasses all activities related to the requisition, order, receipt and payment for materials and/or services from the organization's vendors and suppliers. Activities within most ERP systems that support PTP include:

- Vendor and Item Master Data Maintenance
- Purchase Requisitions and Orders Processing
- Goods/Services Receipt and Verification Processing
- Invoice Entry, Verification and Matching
- Payment and Credit Note Processing
- Sub and General Ledger Updates

As with OTC, there are several configurable controls and functions that should be considered. Examples include:

- ***Purchase Order, Goods/Services Receipt and Invoice Matching:*** ERP systems can be configured to validate purchasing transactions in a variety of ways. Many systems can incorporate a 2-Way, 3-Way or 4-Way match for their purchases and in many cases the type of matching used relates to the type of purchase. For example, compared to direct purchases, indirect purchases are usually handled differently. Therefore, it is critical to fully understand the different types of procurement transactions taking place within the company and the level of matching associated with validating each type of purchase. Oracle can be configured via the Purchasing Option to "Match Approval Level" needed to validate an invoice for payment. The types of options available in Oracle include:
  - 2-Way – Purchase Order and Invoice
  - 3-Way – Purchase Order, Receiver and Invoice
  - 4-Way – Purchase Order, Receiver, Inspection and Invoice

  Within most ERP systems, the matching procedure is only part of the validations occurring prior to the payment of an invoice. The software also can be configured to identify receiving tolerance amounts, which are utilized to determine acceptable variance limits associated with differences between a purchase requisition and purchase order, and/or a purchase order and a goods receipt.
- ***Goods/Services Receipt and Verification Processing:*** It is important to ensure that the inherent risks in this process relative to unrecorded liabilities are carefully managed. Most ERP systems mitigate this risk by recording inventory receipts in an un-vouchered account and subsequently recording vendor invoices in the accounts payable subsidiary ledger when the invoice is received. For example, in SAP, inventory goods received are posted in real-time to what is referred to as the Goods Receipt

(GR)/Invoice Receipt (IR) account for later matching to vendor invoices. This posting process is configurable in most ERP systems, depending on the type of transaction. For example, there are a variety of ways to validate whether a posting is inaccurate or incomplete in Oracle, including:

- Setup of the Purchasing Option for accruing expense items, and setting item validation to "Period End"
- Setup of the Purchasing Option for accruing inventory items, and setting item validation to "At Receipt"
- Setup of the Accounting System Option to automatically create journal entry batches when the general ledger Interface program is run

These configuration settings, when properly set up in Oracle, work to mitigate the risks associated with the posting of procurement-related journal entries.

- ***Invoice Entry:*** Mitigating inaccurate recording of liabilities also is important. JD Edwards can be configured to warn or prevent the accounts payable function from creating a voucher when an invoice number already exists for a supplier. This is done by configuring JD Edwards to perform a vendor-to-invoice match when creating a voucher. PeopleSoft automatically assigns control numbers for critical forms (e.g., receivers, vouchers, check requests, adjustment forms and checks) based on the next available number. These control numbers are key fields to prevent, for example, duplicate payment of vendor invoices.

16. What are some application control considerations for the Close the Books/Financial Reporting cycle?

The financial close process should be configured within an ERP system to assist in addressing risks inherent in subprocesses, such as the processing of journal entries, account reconciliation, closing reports, consolidation and the drafting of financial statements. Some other items to consider within the ERP include:

- Configuration of the organizational hierarchy, chart of accounts, reporting structure and closing of the books
- Frequency of posting of journal entries to subsidiary ledgers and reconciling subsidiary ledgers to the general ledger (Note that some ERP systems post to the general ledger on a monthly basis in batch mode, while other ERP systems post to ledgers immediately.)
- Journal entry configuration options such as "park and post" approvals, posting tolerances and balancing (debits equal credits)

For example, SAP enables controls such as:

- "Park and post" workflow to enable a given user to propose an entry and a separate user to approve the entry
- Functionality to set the timeframe for posting periods
- Clearing tolerances to be established so that only journal entries above a pre-determined threshold are blocked before posting to sub-ledgers and general ledger

SAP also is coded to require that all journal entries balance in terms of debits equaling credits.

PeopleSoft can be configured to integrate sub-ledger activity to automatically summarize and post appropriate entries to the general ledger accounts. This can be accomplished by utilizing the Journal Generator (JG) to create journal entries for each of the subsystems. The JG also may be utilized to set up standard recurring entries. Controls may be incorporated into the JG by defining the control accounts restricted to only allow

posting of journal entries direct from the JG and, in effect, disallow posting of manual journal entries to these accounts. Because the General Ledger (GL) User Preference "Change Journal from Journal Generator" may override this control, this privilege should be granted only on a limited basis when a sound business reason is demonstrated to do so.

The implementation of an ERP can integrate journal entry activity between the subsidiary ledgers and general ledger and, if configured correctly, can significantly reduce the amount of time spent reconciling accounts. Most ERP systems are delivered with standard reports that facilitate and support the reconciliation process. For example, the following PeopleSoft standard reports should be utilized to reconcile sub-ledgers with the general ledger. Example reports include:

- AP Journal Account Summary
- AP Balance By Account/Vendor
- AP Balance By Vendor/Account
- AP Transaction Dtl By Account
- AP Transaction Dtl By Vendor

While reports support the review process, an ERP does not eliminate the necessity to review key balance sheet and income statement accounts as well as processes that require judgment and/or manual intervention (i.e., determination of write-offs and reserve levels). In addition, key processes within the financial close require formal documented policies and procedures.

Section 4: Access Security Considerations

17. What are the principal risks related to access security?

The primary risks relating to access security involve unnecessary, unauthorized, conflicting or excessive access resulting in unauthorized transactions and/or a degradation of the integrity of the underlying application data. Our experience has shown that many security configurations create exposure relating to segregation of duties (SoD) issues and/or excessive access to sensitive transactions due to the following reasons:

- Application security is intended to ensure that the organization's personnel are able to perform only the activities that are necessary to discharge their job responsibilities and to help an organization appropriately segregate conflicting duties. However, we have seen that often during the implementation of a significant application, security is viewed as an enabler instead of as a control. That is, as functionality issues arise and deadlines draw near, many organizations enable increased access to transactions or functions in an effort to facilitate resolution of problems. This problem-solving approach defeats the primary purpose of application security, particularly if sustained post-implementation, as is discussed further below.
- Commonly, prior to go-live, "superuser" access is activated for implementation members who will serve in a support function post-implementation. These individuals utilize these roles to quickly diagnose and resolve problems experienced in the newly implemented application. While the need for these roles is understandable and easily defended, they compromise effective security and represent potentially significant control weaknesses going forward.
- During the implementation of an application, we have seen instances where the proper emphasis was not placed on access controls. For example, the integrator (implementer) relied upon the user or client to define the security settings and role definitions that are necessary to allow for efficient processing. These situations oftentimes err on the side of too much access versus not enough.

- Situations arise where the change control and security administration processes are not robust enough to ensure that the initial intended security design is maintained period after period. Without an effective general security administration process, the specific security controls at the application-level are effectively rendered irrelevant over time.

18. What should be considered when assessing user access rights and privileges for compliance?

Compliance or audit reviews of user access rights should consider multiple elements. These elements include, among other things:

- Evidence of the application and data owners' approval and monitoring of the propriety of the access "touch points" identified.
- Appropriate consideration of system administration access for the transactions being reviewed.
- Evidence that critical segregation of duties rules are not being violated due to personnel access modifications since the prior review.
- Organizational policies regarding access provisioning are being followed.
- Evidence that specific critical transactions were not inappropriately accessed since the previous review.

When performing these reviews, it is critical that the reviewer understand:

- The user access process (i.e., the granting, removal and change of user access rights within the system)
- The roles of the business and IT organization within this process
- The administration of security (i.e., how is security administration different from the user access and monitoring processes?)
- Preventive and continuous monitoring of user privileges and compensating controls
- The ERP security structure as well as any tools utilized to support that structure, such as SAP's Profile Generator

If changes are needed based on these reviews, a standard process should be in place to ensure these changes are handled in an expedient manner. If there are findings in the access security area that evidence a breakdown in the security administration process, a root-cause analysis should be undertaken and the matters resolved on a timely basis.

Numerous software vendors have developed automated solutions to assist in the implementation, testing and maintenance of specific security rules. Some of these tools are discussed further in Section 10 of this document.

19. What processes should be in place with respect to establishing proper user access security and segregation of duties?

At least four steps should be considered in establishing proper user access security and segregation of duties:

1. ***Define:*** User access rights must be defined in terms of business functions that a person must perform according to the performance expectations articulated in the description of his or her job responsibilities. Where segregation of duties conflicts exist within a person's job role, these should be resolved or mitigated via compensating controls before translating these job functions into system privileges. As job roles are created within the system, segregation of duties concepts should continue to be applied within the context of how ERP logic is used to create user privileges. Refer to Question 26 regarding SoD concepts within ERP logic.

2. ***Test:*** User access rights should be tested within the system from "a functional view" through unit testing (i.e., does the system allow or disallow the specified functions to be performed), "a user view" through user acceptance testing (i.e., the user logs into the system using their assigned privileges and confirms or denies that the rights meet the requirements specified in the definition stage), and "a controls view" through control testing (i.e., do the rights of the user comply with the access security and segregation of duties specifications established in the definition stage).

3. ***Implement:*** User access rights should be implemented according to what is approved in the definition and test stages. Implementation of user rights may occur several times throughout the system development lifecycle and in the succession of system environments (e.g., development, test, quality and production).

4. ***Monitor:*** After access rights are implemented in a system environment, they should be monitored to ensure they are performing as specified. Activities related to maintaining proper user access security and segregation of duties are discussed throughout the following questions.

20. What processes should be in place with respect to periodic review and approval of access to critical and/or sensitive transactions and data?

As part of their responsibilities, application and data owners should oversee periodic reviews to determine who has access to critical transactions for which they're responsible. Their reviews are intended to ensure that only those individuals with a legitimate business need are authorized and able to execute and/or view critical transactions and data. While the frequency of the reviews should be based on the criticality and sensitivity of the transactions and data being reviewed, we recommend they be performed at least quarterly.

Typically, this oversight process involves reviewing a list of current users with access to a specific transaction or set of transactions. For instance, the purchasing manager might review listings of all users with access to generate purchase requisitions and purchase orders. In this review, the purchasing manager should look for:

- Users who should no longer have access to these transactions based on a position change, such as transfer or promotion or who are no longer with the organization.
- Users who may represent a segregation of duties conflict, such as an individual from the receiving dock or a member of the accounts payable department.
- Unknown users who may have received access inadvertently or inappropriately.

Exceptions identified during this review should be investigated and corrected immediately. Consideration also should be given as to whether or not security administration procedures need to be modified to prevent the noted exception from occurring again. In addition, evidence of the review and corrective action taken should be retained for subsequent compliance review efforts.

The aforementioned review and approval process can be automated via use of some of the tools discussed in Section 10 of this document.

21. What are the roles of the business and the IT organization in controlling user access processes and segregation of duties?

In the past, it often was perceived that the IT organization owned or was responsible for access rights pertaining to business users. Current trends suggest that, while IT plays a critical role, it is primarily a business responsibility to ensure that management of user access activities (i.e., authorizing and initiating additions, modifications and terminations to user access tables) does not result in inappropriate conflicts or access to sensitive information. In complex ERP systems, IT personnel can provide critical expertise on how best to establish and build user access profiles according to the organization's business requirements.

While IT departments should ensure employees in the IT group have adequate access consistent with sound segregation of duties principles and appropriate limitations on access to sensitive functions, these employees should not be responsible for interpreting business user access requests for propriety. Specific rules related to

segregation of duties and limited access to sensitive functions should be defined and regimented in such a way that security administration personnel can effectively check access requests (against these rules). The objective is to avoid placing security personnel in a position of making decisions as to the legitimacy of specific requests. Procedures should be defined for: (1) handling authorization requests which compromise the defined rules, (2) obtaining appropriate approval of specific exceptions and (3) modifying the requested access in such a way that the defined rules are not compromised. Procedures also should be in place regarding notification of management personnel for identified compliance exposures due to a user's system privileges.

22. How can an organization improve its ability to manage appropriate security without incurring excessive cost and time bottlenecks?

Some organizations have adopted "80/20 models" that incorporate pre-defined, pre-approved user access roles. The 80/20 model implies that 80 percent of the user administration activities will be within the standard model and require little to no manual intervention. For example, a fixed assets manager requesting access for a new employee who will be a fixed assets clerk will be within the standard model. Security administration personnel or tools would automatically enable the standard fixed asset clerk role to this individual without specific approvals, consistent with the predetermined functions required by the job specifications for that role. However, if the same individual requested access to the accounts payable clerk role, additional approval would be required.

If nonstandard requests represent more than the anticipated volume of activity, this may be an indication that security structures are not well configured or business user requirements were not well defined during the implementation process. It also may be an indication that users are not clear as to the types of rights their job function entails, how their functions may be performed in the system or why specific limitations may be necessary.

Therefore, nonstandard requests can be classified as requests that may compromise segregation of duties and restrictive sensitive access privileges. Sometimes these requests are warranted due to lack of personnel required to perform a particular function in addition to the normal activities. Mitigating detective controls are critical to maintaining a good overall control environment in these cases.

Additional security approaches such as single sign-on, coordinated security administration across application(s) and infrastructure(s), and automated security administration tools also can help an organization better manage this process. For more discussion on the automated tools, see Section 10.

23. What is the best method for organizing user access authorization rules?

Today's best-practice model is to use role-based access control (RBAC), an operational model for the implementation of privileges in complex system environments. Instead of determining exactly which privileges are needed by each and every individual, and adjusting those privileges as circumstances and job responsibilities change, privilege and access levels are assigned to specifically named roles, and then these roles are assigned to users based on their job needs or areas of responsibility.

Roles must be carefully implemented such that no role has excessive privileges. Furthermore, because individuals are normally given the use of multiple roles, the sum total of privileges across all of an individual's roles must be evaluated to ensure that proper segregation of duties is maintained.

Unfortunately, the complexity of many applications, especially ERP systems, often has exceeded the ability of IT to implement appropriately robust segregation of duties controls. Furthermore, while most of today's ERP products support RBAC, they vary in their granularity. Few, if any, provide proactive modeling of segregation of duties violations before assigned roles are implemented, or identify existing segregation of duties violations.

For this reason, many organizations are turning to add-on software products that provide automated, integrated assistance with role analysis, definition, testing and provisioning. For more discussion on these tools, see Section 10.

24. What other control elements should be considered regarding powerful authorities and systems administration duties?

Superusers also can be termed "power-users" and "privileged-users." These types of user access privileges entail access to sensitive functions or even all-powerful administration rights within an application. Historically, control over these accounts have focused on providing such rights to only a very few "trusted" employees. Within the current regulatory environment, companies and their external auditors are finding it difficult to comfortably rely on this soft control.

Systems administration personnel typically have access to sensitive functions within the application (e.g., table edit, security administration, batch job execution, etc.). As noted in Question 21, it is important that IT management ensures that access to these sensitive functions is appropriately limited. For example, an IT department with 10 people should not simply assign full system access to all 10 individuals "just in case" somebody needs it. Careful consideration should be given to define the specific roles and job duties of each member of the department and application access should be granted accordingly. Additional compensating controls, including transaction logging and monitoring and manual approvals to perform specific transactions, should be considered when assigning these powerful authorities.

One common approach to limit the ability of these users to compromise intended system controls is to use a "library" process. This process includes "checking out" and "checking in" sensitive functions on an as needed basis instead of including these authorities in the users' standard profiles. Approvals of "checkouts" and monitoring of functions are crucial to making a library process sufficiently robust. Another method is to arrange for superuser activity to be monitored by an independent party. Because both methods are difficult to sustain manually, companies have adopted technology aids such as those described in Section 10 of this document.

25. Does security maintenance have to go through the change management process?

Depending on the control environment and standard operating procedures defined by the organization, user provisioning (the assignment of individuals to security roles) typically falls under security administration procedures rather than change control. However, it is advisable to run changes to the security roles through many of the activities of the change management process. Role changes should be reviewed for impacts, approved by management, and tested before they are moved to production. Refer to Section 5 for further discussion regarding change management of general controls.

26. How does the organization assess ERP security structures for compliance exposures due to segregation of duties and sensitive access?

Before evaluating the system for security exposures, the compliance team must first determine the potential conflicts to assess and the conflicts which are inherent in the organization's structure. For example, if there are very few employees in a warehouse, then the receiving and physical inventory functions may be shared by a single employee, whereas in larger organizations these functions may be separated. Typically, organizations assess conflicts within business cycles, (e.g., Purchase to Pay), where a person should not have access to create vendor data and also pay vendor invoices. However, consideration also must be given across business cycles, (e.g., a person should not be able to enter both a sales order and a purchase order). Analysis within and across business cycles must consider corporate policies and procedures. Some organizations take a liberal approach to the data their employees may view, while others may take a more restrictive approach.

In order to identify potential conflicts, the organization should identify which system access rights are important, i.e., the "sensitive access" points. Typically, there are many types of access rights possible within an ERP. By identifying and prioritizing these functions according to the specific needs and policies of the organization, the compliance process can be better streamlined.

The next step is to consider the combinations of sensitive access rights which represent conflicts. If these combinations are assessed at the job function level, this assessment becomes a validation activity to confirm job role definitions using user access rules. Combination assessment tasks within this detailed phase are highly

dependent on the ERP installed. For example: SAP uses a methodology where a user ID is mapped to specific roles/profiles, which consist of transactions utilizing specific authorizations. Authorizations dictate what a user can actually do with respect to that transaction (e.g., read, modify, create, etc.). Therefore, while analysis at the role or transaction levels is significantly easier, without assessing the specific authorization objects, a full understanding of the user's actual privileges is not possible.

SSA Baan users are given a set of permissions that consist of qualifiers. The most critical qualifiers are termed "sessions." Sessions are defined as maintain, display and print; however, table authorizations must be assessed to determine what a user may perform. For example, "Maintain Sales Orders" is session code tdsls4101m000. This session code's table authorization, as it relates to a single user in question, may be set to "read," meaning the user cannot maintain sales orders despite having access to that session code.

For both SAP and Baan, the compliance team must look at authorizations in the context of the particular ERP to determine what functions a user may perform in the system and, based on that review, what real segregation of duties conflicts exist. This approach requires a detailed knowledge of the application functionality, and specifically, knowledge regarding critical authorization functions.

27. What control principles should be considered during an assessment or a redesign of security in an ERP?

Fundamentally, all control processes depend upon a healthy check-and-balance between the protection of assets and the enablement of business activities involving the exchange and conversion of those assets. Adequate segregation of duties is an important consideration in determining whether control activities are effective in achieving the objectives of internal control, especially in conversion cycles. The basic idea underlying segregation of duties is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated include:

- Custody of assets
- Authorization or approval of related transactions affecting those assets
- Recording or reporting of related transactions
- Execution of the transaction or transaction activity

An essential feature of segregation of duties and responsibilities within an organization is that no one employee or group of employees has exclusive control over any transaction or group of transactions. The primary means by which to assess the segregation of duties around the exchange or conversion of assets between multiple persons includes ensuring appropriate handling of transactions through effective peer controls and upstream or downstream verification checks. Examples of peer controls include dual signature approvals, exception/summary reports, and supervisor review and approvals. A lack of segregation of duties can often appear to be an adequately controlled environment since related processes or events happen at different times, including batch processing or access controls over application processing tools. In addition, when no one performs a duty, it may indicate a control weakness.

It is common knowledge that company size can affect the feasibility of segregating incompatible functions. Some small processing or accounting departments may not be capable of enforcing adequate segregation of duties in their system, and, therefore, rely on other mitigating controls to ensure transactions are handled properly. For example, a few accounting clerks may be responsible for recording and executing transactions; however, a supervisor receives transaction activity reports, reviews batch details, controls system access and performs additional reconciliation activities to enhance oversight. All such mitigating controls and related evidence of performance can maintain adequate control environments. Nevertheless, they should be carefully examined from time to time as circumstances change.

28. How does management decide whether to remediate individual security and segregation of duties problems versus reengineer user access overall?

Many companies have found that reengineering user access in their ERP systems provides a better return on investment than trying to fix the user rights that currently exist. Redesign begins with recognizing this procedure as an option and assessing the state of current ERP security in meeting compliance goals. If the need to restructure is significant, it may be better to begin with a clean slate and redesign security as if the situation is an initial implementation. This often reduces ongoing maintenance costs, time and effort rather than trying to apply patches of rework to the existing security structure that may not be sustainable and satisfy compliance requirements over time.

29. What is an efficient way to document segregation of duties and sensitive access?

Generally, we recommend documenting segregation of duties (SoD) and sensitive access in separate Risk and Control Matrices (RCMs) as opposed to having them embedded within business process RCMs. This approach leads to increased clarity during the performance of design assessments and testing of these areas.

In organizing documentation, we recommend sequencing SoD and sensitive access according to the steps in which a process occurs. For example, within the Revenue Cycle (Order to Cash), customer master data combinations are analyzed against:

1. Inquiries and Quotations
2. Pricing and Contract Management
3. Sales Order Processing
4. Shipping – Delivery – Return
5. Accounts Receivables – Billing – Invoicing – Credits – Cash Management

If the RCMs follow the same structure as the corresponding business process, easy reference is facilitated to enable an understanding of the mitigating controls for specific access exposures. See Section 7 for further discussion of documentation concepts.

30. Can automated tools be used to assess segregation of duties and sensitive access for compliance exposures and provide ongoing monitoring?

To enable assessments of sensitive access and segregation of duties, many companies are turning to automated tools. These tools often provide better clarity, accuracy, repeatability and time savings when assessing user privileges. They come in a variety of packages and have unique advantages and disadvantages depending on the functionality the organization values most. If a tool is implemented as an "Enterprise Solution" where it is used to manage user access processes and rights, it becomes a key control for the purposes of SOA Section 404 compliance. Thus, the rules and workflows within this enterprise tool should be tested independently to verify appropriateness and accuracy. Refer to Section 10 for further discussion of automated tools.

Section 5: General IT Controls Related to Applications

Protiviti's published *Guide to the Sarbanes-Oxley Act: IT Risks and Controls* is a companion to the latest edition of Protiviti's Section 404 guide and is available on **protiviti.com**. We have included relevant content from this publication below for emphasis and, in some cases, have expanded upon the content to provide more specificity regarding the relevance to Sarbanes-Oxley Section 404 compliance.

31. What does the Section 404 compliance team look for when evaluating application change controls?

Background

The application-change process is one of particular significance to internal control over financial reporting. The integrity of application changes directly impacts the accuracy, consistency and completeness of transaction processing, as well as the accurate and timely accumulation, summarization and reporting of transactions.

As companies change their application systems, the risk emerges that the changes may cause applications to lose their integrity. This creates a potentially substantial risk of inaccurate, incomplete or otherwise incorrect processing affecting financial reporting. Because of this financial reporting-related risk (as well as other obvious strategic and operational business risk issues), companies must have a well-designed and effectively operating application change management process. Proper change control procedures are a critical element of an effective change control process and part of an overall baselining testing strategy, as discussed in Section 2.

Change control procedures should cover all aspects of the change cycle, including initiation, monitoring, testing and approval, as well as migration of the appropriately approved change into the production environment. This process also must be appropriately secured so that personnel in this function cannot, without detection, make inappropriate changes to the program or the related data. The change process must be comprehensive in nature, considering all possible implications of the changes, such as systems interfaces, data and error-checking routines, application security changes, management reporting, etc.

Impact on financial reporting assertions

a) Application changes directly impact the completeness, accuracy and consistency of the applications that process transactions and summarize and classify accounting information and disclosure.

b) Application changes can affect the appropriate segregation of incompatible duties when changes are made to add or modify duties and/or impact access to sensitive transactions and data.

c) Access to information assets may be made available to unauthorized individuals through the change control activities.

Impact of strong controls

a) Application functionality and controls can be relied upon to consistently operate as intended by the users. Change control directly affects the control assertions around the completeness, accuracy and consistency of processing and enables a successful baselining testing strategy, as discussed in Question 7.

   A word of warning: These controls assure the application functions as designed and intended. The control considerations within each application also must be evaluated to determine whether the application's design provides for all the necessary controls to perform and achieve reliable financial reporting.

b) There is assurance that the change control process has not compromised the integrity of the data.

Impact of weak controls

a) There is no assurance that modifications to the programs have not adversely impacted the intended programmed controls. As a result, compensating controls would need to be evaluated and documented. These compensating controls generally should be manual and detective in nature, and may need to be performed at a fairly detailed level. In addition, there may be a need to further investigate the changes made to critical programs (e.g., the nature and frequency) in order to understand the particular types of controls required to detect specific errors that may arise if changes to the applications were not appropriate.

b) If access to applications and production data has not been appropriately restricted during the application-change process, there would be a need to consider and document the compensating controls necessary to detect inadvertent or intentional changes to the data or programs.

c) All critical application controls (e.g., configurable controls and security settings) would be required to be tested each year as part of the SOA Section 404 compliance effort, as opposed to simply testing the change control process and those controls that have been modified during the current fiscal year.

32. What elements of data management and disaster recovery should be evaluated by Section 404 compliance teams as they relate to applications?

According to clarifications provided by the PCAOB in Audit Standard No. 2, Appendix C5 (Release No. 2004-001), business continuity matters are not directly in-scope for Sarbanes-Oxley Section 404 requirements. The PCAOB is only addressing this matter in a very narrow compliance sense. The Board is not passing judgment on the business merits of managing the risks around business continuity. Our point of view is that proper attention to business and systems continuity is appropriate for a variety of operational and reputation reasons. See Protiviti's *Guide to Business Continuity Management* (available at www.protiviti.com) for helpful insights to address these critical matters. Hurricanes Katrina and Rita demonstrated the pain that organizations can face if ill prepared, including impacts to financial reporting. We are also aware of "near misses" in which a catastrophic event placed a company at risk of not meeting its public reporting deadlines.

In contrast, data management is clearly an expected element of any comprehensive compliance plan, particularly with respect to ensuring the company's capabilities to file accurately and timely its required financial and other reports with the SEC under the Commission's rules and regulations. For purposes of this discussion, "data management" relates to the processes around the backup, recovery and restoration of data. Current and available data is the lifeblood that keeps applications healthy and useful to the organization. The company must have the ability to restore or restart its processing in a manner such that it does not lose the integrity and completeness of transactions or data.

The focus for data management should consider the criticality of the application, and therefore, the appropriate timing and frequency of the back-up process. Provisions such as off-site storage and periodic restoration testing also are important to ensure that data can be efficiently located and restored to the appropriate application if a need arises. It is further advisable to retain backup "snapshots" from important time gates such as quarter and year-end for longer periods, consistent with the organization's document retention policies.

33. What elements should be considered with respect to the network, operating system and databases to support effective application control?

Protiviti views risks to information processing through a hierarchy of technology layers. As already established throughout this publication, good controls within the application functionality support a well controlled business process. Similarly, good controls over supporting databases make possible an effectively controlled application, and so on. The following is a set of representative examples from the infrastructure layers that should be reviewed with particular attention to the general controls area of the compliance process. These are not a complete listing.

Database (Oracle, SQL Server, DB2, etc.)

- The primary security concern here is that the security objectives and controls germane to the application layer are not undermined by those capabilities available in the underlying database layer. For example, direct connections to database tables that circumvent the logon procedures of the application should be carefully restricted.
- Changes to the database structure for most ERP systems are prohibited by the vendor, except for the addition of custom tables. Access to create tables also should be carefully restricted and run through the change control process.
- Stored procedures and batch jobs that automatically update or transform data (aggregate, re-calculate, delete, etc.) should be carefully tested and managed through rigorous change control processes.
- Similar to application superusers, database administrators (DBA) have powerful rights to database content and therefore should be limited in number and, if feasible, monitored for unauthorized data change activity. Often, companies require that "data fixes" by IT professionals/DBAs go through a change control channel with proper business approvals before such changes are put into effect.

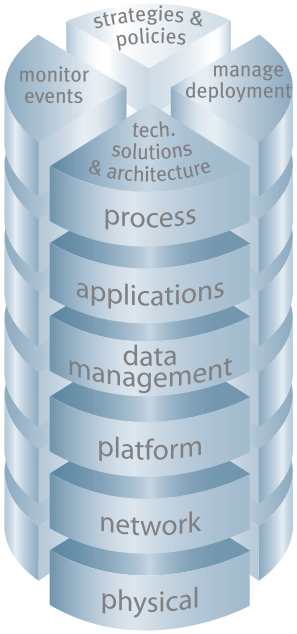

Figure 3

- Certain static tables or configuration options may warrant special logging or audit trails due to their particular risk impact. The scope of database logging must be carefully considered to avoid unacceptable performance drains on processing speed and disk space.

Platform and Network (Windows, XP, UNIX, etc.)

- The operating system (OS) of the application or database server contains inherent risks that must be controlled. Updates to OS versions are crucial in keeping up with the ever-changing security vulnerabilities today. However, updates should be individually evaluated and tested prior to rollout to ensure compatibility problems with the database or application are flushed out.
- Servers upon which the applications depend should have proper virus detection and prevention protections.
- Applications often output to or are fed by files in network directories (file share). Therefore, from a chain of custody perspective, the security objectives required for the data while in the application should also exist at the directory level. In practice, these objectives require the identification of key directories and a periodic review of users with rights to the critical files within those directories.
- Increasingly, companies are looking to reduce the number of passwords that employees must remember by utilizing technologies such as Microsoft's Active Directory identity management solution. In essence, single sign-on reduces the risk of passwords pasted on keyboards, but also eliminates the multiple barrier protection afforded by dual authentication to the network and application layers. Therefore, in these environments, it becomes crucial that the password requirements and other user management controls described in Section 4 be fully absorbed into the network level controls.

Physical

- Access to the data center or locations in which the servers physically reside should be carefully limited to avoid security tampering and equipment interruption.
- The equipment upon which the applications depend should be kept optimized with prudent upgrades and disk space expansion as necessary to maintain operations and avoid data corruption.

34. What are interface risks and how are they managed?

Interface risk is present when external and internal interfaces are not properly specified, defined, designed, documented and monitored. Such interface risks often lead to the inconsistent reconciliation of sent and received data, resulting in unidentified errors in the data. Effectively designed interfaces will prevent and detect these errors at the earliest possible point in processing, facilitate error correction and employ appropriate user controls. When properly structured and documented, interfaces will aid in cost-effective maintenance and recoverability.

Interface risks can be managed by securing data from unauthorized modifications; transferring data in a timely, accurate and complete manner; and performing error resolution procedures accurately and timely. Further, the receiving system should process data more than once as a method for managing interface risks. The following chart lists examples of specific control objectives and the related risks and controls.

CONTROL OBJECTIVE	RISK	CONTROL
Application controls are adequate to prepare or process sent and received data	Inadequate controls could prevent accurate and timely availability of information to both application and legacy application users	• Once the application receives data, it is converted to the appropriate format; converted information then enters the session and errors are logged • Errors are resolved and resent, and resolutions documented and approved • Unresolved errors are reported to the interface owner
Restart and recovery procedures for interface sessions are appropriately established to ensure timely resolution of interruptions in transmitting files between systems	Inadequately designed restart and recovery procedures may cause undue delays in processing and lead to unnecessary and costly use of personnel time	• Interface sessions use an application having its own restart system in the event that a connection is broken • The application also uses a checkpoint system during file transfers; this system is configurable and will verify data transfers between target and source locations • Transfers that are stopped or fail prior to completion automatically resume, continuing from the last checkpoint
Data that has been transferred between applications is tracked and monitored to ensure errors are resolved appropriately or escalated as needed	Manual input of data is vulnerable to human error; without adequate tracking and monitoring, errors may go undetected	• Regular edit checks, including reconciliations, are responsible for catching invalid data before an interface file is created

In addition, the design of the interface should ensure an appropriate mapping of source data to a destination application or data table, as well as an assessment of the data as it relates to the level of detail required for use in the destination application.

Section 6: Implementation Controls and Considerations

Major changes, such as the implementation of a new application or upgrade to an existing system, naturally introduce a heightened level of risk. The controls that have been discussed for existing systems also should be considered for new or updated systems. However, unique risks emerge that require particular attention.

35. What are the primary risks of implementing a new application, and how are they managed?

The primary risks related to the implementation of an application can vary widely based upon many factors, including the complexity of the application, the size of the organization, the purpose of the application and the scope of the implementation.

As part of any significant implementation, a formal implementation risk management methodology should be employed to ensure the identification, prioritization, measurement and proactive management of the risks inherent in the implementation. The methodology should include the following steps:

1. Form an Implementation Risk Management Team comprising senior individuals whose roles and responsibilities enable them to assess risk across the implementation.
2. Define relevant risks to the implementation using a customized Implementation Risk Universe (see below for examples).
3. Prioritize the risks in the Implementation Risk Universe based upon likelihood of occurrence and significance to the organization.
4. Develop risk management action plans and implementation controls for mitigating high priority risks and incorporate them into the overall implementation plan.
5. Define metrics for each high priority risk that allow for periodic monitoring of the extent of the existence of the defined risk.
6. Assign risk management responsibilities among the Section 404 compliance leadership and the members of the Implementation Risk Management Team; conduct specific risk and control awareness training.
7. Execute the risk management action plans.
8. Monitor risk metrics as part of project management, and conduct regular check points to ensure that the risk management action plans, as defined above, effectively address high priority risks.

An organization's Implementation Risk Universe can be categorized into Project Management Risks, Process/Technology Risks and Information Risks.

- **Project Management Risks** typically relate to project components such as:
  - Project scope
  - Staff resources, including availability of necessary skill sets
  - Reliance on third-party expertise
  - Roles/responsibilities, both during the implementation and subsequent to go-live
  - Project timeline and progress
  - Issue identification and response
  - Team member turnover during/after the project
  - Implementation communications and expectations management

- **Process/Technology Risks** include such categories of risks as design, alignment, architecture, deployment, security, change management, support and data integrity. These risks typically relate to implementation components such as:
  - Requirements management
  - Process design
  - Functionality design
  - Product customization
  - Program change/version control
  - System and configuration data control
  - Standing/master data control
  - Transaction data control
  - Interfaces
  - Security architecture
  - Functional testing
  - Data conversions
  - End-user acceptance
  - Responsibility transitions
  - Training and roles
  - System cutover/go-live
  - Scalability and reliability
  - Access administration
  - User support
  - Operational support (backup, batches, etc.)
- **Information Risks:** New systems typically deliver new information sources that are utilized for decision-making and reporting and oftentimes result in reengineered processes. Additionally, implementations themselves should generate certain documentation that should be retained. Information risks, which should be identified, prioritized and managed, include those relating to:
  - Performance metrics
  - System documentation
  - End-user procedures
  - Baseline documentation (evidence of proper operation of key functionality)
  - SOA 404 compliance documentation and Section 302 compliance enablement
  - Operational, management and financial reports
  - Queries and other information sources from the system

36. What are the primary risks relative to data conversions relating to an implementation, and how are they managed?

The following high-level steps are appropriate to identify, assess and manage risks relating to the data conversion process. The old adage remains very true – no matter how well the application performs, "if you put garbage in, you will get garbage out." Therefore, the data conversion component of an implementation deserves attention to ensure that the important risks are reduced to an acceptable level.

Plans and procedures to convert historical and standing data from the previous application (the source) to the new application (the destination) should incorporate the appropriate controls. Similar to chain of custody requirements in investigations, data should be carefully extracted, analyzed, transported and applied without ever harming the accuracy and completeness of the record. There should be procedures and checkpoints throughout the process to identify if something has been lost, corrupted or manipulated. Conscientious personnel should be accountable to monitor that these checkpoint controls are carried out with diligence and precision. The formality and sophistication of techniques to execute these steps depend on a variety of factors, such as the size, complexity and transportability of the data to be converted.

The following steps are modeled after the traditional batch extract, transform and load approach. However, the spirit of the control recommendations can be applied to many forms of conversion.

1. ***Extract the right data out of the source system:*** A careful analysis of current data elements required for conversion should be undertaken, including an examination of the data types, common values and counts. A baseline snapshot of current values and balances to be converted should be captured for subsequent comparison. A few particular data elements should be identified as control fields to allow for periodic checks of completeness as the conversion unfolds. These control fields often take the form of a unique data element such as "Record ID" or an important financial element such as "Sales." Using conversion tools, data tools or native queries, the records should be extracted and compared to the baseline to ensure all records and elements are obtained before proceeding to the next step.

   If necessary, existing data should be cleansed for duplication, aged data, and other errors prior to extraction.

2. **Carefully transform the source data to a meaningful format for the destination system:** Except for upgrades, the format and field designations between source and destination systems usually require a mapping exercise to link what the field used to be to what it must become. The accuracy and coverage of this data mapping is extremely important to not only ensure that the data comes across, but also, that each element lands in the right place. Business user review and sign-off of mappings are a key success factor for accurate conversions and user acceptance conversion results.

3. **Methodically load the reformatted data into the destination system:** Numerous trial runs of conversion programs and procedures should occur to work out any issues on conversion logic and events. The sequence for loading various data sets should be carefully planned and executed to accommodate data interdependencies and linkages (such as vendor master before purchase orders). After loading, control fields in the destination system should be compared to relevant fields from the source system to confirm that conversion has carried over all of the expected records. Inevitably, there will be some data that could not be fully applied through the primary conversion process. These data are typically handled through manual "data-fix" procedures, which should incorporate the same level of completeness and accuracy controls as the rest of the conversion.

4. **Obtain user/management acceptance of the conversion:** Most of the system and IT-based controls for the conversion activity relate to the completeness of the data transferred (i.e., did all fields and all records make it across?). There also are some systematic comparisons that are used to conduct checks on certain value sets to verify that the content retained its accuracy. However, the burden for accuracy primarily rests with the designated user or business management. These parties are called upon to carefully review comparison reports to identify flaws in the data set and review commonly used reports from the new destination system to identify any data compatibility problems and obvious errors and omissions. To make this exercise more than a cursory glance, it is recommended that user acceptance take the form of a formal sign-off with real accountability behind it.

5. **Retain conversion documentation:** Because financial records are the basis of a fair and accurate representation of a company's financial position, data conversions will be an intense focus for internal audits, external financial audits and Sarbanes-Oxley compliance. Therefore, it is imperative that all artifacts proving the accuracy and completeness of the transfer be retained for future review. Examples include pre-conversion snapshot reports, the comparative post-conversion reports, data maps, sign-off and acceptance forms, testing/verification documentation, and conversion program change control information.

It also should be mentioned that impacts of the conversion on other applications and their interfaces should be carefully considered. Changes often must be made in these interdependent components to accommodate new data characteristics in the replacement system.

37. What are the risks to functional testing when implementing a new application, and how are they managed?

When new applications are implemented, extra care must be taken to ensure that the testing of automated process controls (see Section 8) is sufficient to verify that the application is configured to provide the intended results as well as prevent or detect unintended results. Therefore, organizations must apply appropriate techniques to provide both positive and negative assurance. These types of tests are discussed further below:

- ***Positive Assurance*** involves testing to confirm that the control or function is operating as intended. An example would be processing a transaction in a foreign currency and confirming that the transaction is accurately translated to the domestic or functional currency, and accurately posted to the appropriate accounts. An example of this type of test would be to confirm that a purchase order over $500 will post with appropriate approval.
- ***Negative Assurance*** involves testing to confirm that unintended results of a control or function are not encountered. An example would be attempting to post a journal entry that does not balance in order to validate that an error message is displayed, precluding the processing of the journal entry. A related example of negative assurance testing would be to confirm that a purchase order over $500 will not post without appropriate approval.

Section 7: Documentation

Documentation is important in an evaluation of internal control over financial reporting. Our responses to the questions in this section provide guidance on documentation at various levels, including the entity level and activity/process-area level. Documentation of IT risks and controls needs to be consistent with the overall standards and approach set by the Section 404 compliance team. Documentation also must satisfy the requirements of the attestation process.

38. How should the Section 404 compliance team document the IT controls addressing the processes controlled by application and data owners and for the specific application areas?

For the processes controlled by the application and data owners, we believe that process maps and risk-and-control matrices are the most appropriate tools for documenting the processes. As noted in Section 2, at the business process level, the documentation of the application-level controls is best accomplished in an integrated fashion with the other business process risks and controls. In fact, integration is the best way to fully understand the dependency of internal controls on IT. It may be helpful to indicate when a business process control is an application control so that they can be reviewed and tested, as necessary, by an individual with application control expertise. There should be additional documentation around key applications such as system maps or data flows, matrices that indicate applications impacting the business process, and a matrix of key application control considerations. The key control considerations would highlight complex calculations, key data validation and verification checks, significant and/or complex interfaces, etc. Accordingly, the appropriate skill set must be brought to bear.

39. How much documentation should the IT organization and the application and data owners have in place to evidence the controls and functioning of a critical application?

There are two considerations related to this question. The first relates to the documentation needed to evidence the effective functioning of the application program and its related controls. The second addresses the technical documentation necessary to ensure that the application can be maintained such that the integrity of the processing and controls can be assured.

Application documentation should specify where and how key components of the application operate. The key components should include the critical application controls discussed in previous questions. The documentation can take many forms, including process flows and narratives, flowcharts that show the steps during program processing, and other technical documents that show data relationships and database designs.

The technical documentation should be granular enough such that an unfamiliar (but technically competent) programmer could understand the program functionality, and its critical interfaces, data handling and security features. The documentation should provide a reasonable basis for performing the required maintenance.

Documentation which includes only the base program code and technical database specifications is not considered adequate in most circumstances. If there is inadequate documentation of the application, it increases the risk that changes may not be appropriate. If that risk exists, the implications of weaknesses in change management should be considered.

40. Given the emphasis placed on the "initiating, recording, processing and reporting" of transactions by the PCAOB in Auditing in Standard No. 2, what is the best way to document transaction flows?

We believe the best way to document transaction flows is through application and data-flow diagrams. These diagrams provide a picture of the significant data flows through the company's various applications from the point of origin until they ultimately affect the financial statements and disclosures. We believe there is a need to begin these diagrams initially at a high level and then provide more detail for the most significant transactions and applications. In the more detailed diagrams, it is useful to highlight the inputs, processing activities and outputs, as this demonstrates the understanding of the "significant business processes" that the PCAOB requires the external auditor to attain through walkthroughs.

Section 8: Testing

Like all other controls, IT controls must be tested to ascertain that they are operating as designed. The third edition of our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* provides detailed guidance on testing. We have included relevant content below for emphasis and, in some cases, have expanded upon the content to provide more specificity relating to testing of application-based controls.

41. How are IT controls tested?

IT controls should be tested in a manner similar to the controls in other process areas. There should be appropriate use of inquiry, inspection, observation and reapplication and/or reperformance testing techniques. In all instances, adequate documentation of the testing should be developed. A combination of testing techniques is often appropriate to form a conclusion related to operation effectiveness.

At the IT entity level, one would expect most of the testing to be related to inquiries, inspection and observation because reperformance and reapplication cannot typically be accomplished for many of these types of controls. For the processes in the general controls area and for application and data-owner controls, there is a need for all four types of testing, including reperformance and/or reapplication. For these processes, the process-level control design ordinarily should provide for evidence that certain parts of the process were completed (e.g., signatures or other sign-offs on forms, etc.).

42. Who should test automated controls?

Automated controls should be tested by the business process owner with internal audit present during the testing. These controls are usually configured to affect either how entries are approved or the processing of specific business data. In most cases, the internal audit IT team will not have the business process knowledge to successfully execute a test that triggers the automated controls. It is therefore important that the individual testing the automated controls understands the business process being tested, the automated controls involved, the purpose of those controls, and how the system should react when the controls are triggered. Organizations should consider involving application control specialists to ensure effective and accurate testing. In Question 43, we address the use of automated testing tools to improve the efficiency of configured controls within an application.

43. How are application controls tested?

Question 3 provides detail on six different types of controls relevant to business applications and the transactions they process. Effectively testing the application and the processes it supports requires a mix of testing methods and techniques. Below, we consider two of the control types most commonly referred to as "application controls": automated process controls and application security. Generally speaking, the two primary methods to test these application controls are automated tools (discussed further in Section 10) and manual verification techniques.

- **Manual Testing:** Often, this method is considered the "easiest" approach. However, this method is typically very time-consuming and difficult to perform due to the number of controls to test, as well as the number of scenarios requiring the gathering of sufficient evidence to validate that the control is operating effectively. In addition, as further discussed in Question 37, tests must address both positive and negative assurance. Significant skill sets and knowledge capital are often required to build relevant test cases, appropriately execute tests, interact with business personnel and accurately interpret test results. The manual testing approach often requires access to a synchronized (i.e., mirrored) environment to ensure that evaluators are not inappropriately accessing or impacting the production (live) environment. Finally, as with any action performed by people, there is always an increased risk of human error. These difficulties do not preclude effective use of manual testing techniques. In fact, many organizations successfully deploy manual testing techniques in their environment. In many of these organizations, however, we have seen significant opportunity to reduce the overall testing effort and improve its effectiveness through increased use of semi-automated and automated techniques. These techniques are discussed further below.

- **Semi-automated testing via data/table extraction and analysis:** For some applications, the organization may have the ability to extract data tables, which serve as evidence that a particular set of controls has been configured in a certain fashion. In some cases, auditors may want to manually "scope test" a sample from the data table to confirm that what is indicated by the table is actually configured and operating effectively within the application.

- **Automated testing:** In many cases, automated tools may be available which can augment and improve an organization's testing effort. Some of these tools can be set up to pull configuration information from the application and analyze the data automatically against defined, anticipated results. Some tools enable an organization to define business rules at a transaction level that serve as evidence of the operation of a particular configurable control. Finally, rule-based "continuous monitoring" tools exist in some cases that enable an organization to monitor for changes in pre-defined configurations and for specific types of transactions that indicate increased risk to the organization. These tools enable much broader coverage than conventional manual testing approaches.

The use of an automated tool is not a "silver bullet." As with any application, the early stages of implementation and use often are challenging, requiring attention to detailed customization requirements, knowledgeable skills and experience, and familiarity with testing objectives. However, if configured correctly and utilized by individuals with the right expertise, these automated tools can add significant efficiency and value to the assessment process. For more discussion of these tools, see Section 10.

Section 9: Addressing Deficiencies and Reporting

If there are internal control deficiencies, they must be remedied if significant. The third edition of our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* provides guidance on addressing internal control deficiencies. We have included relevant content below for emphasis and, in some cases, have expanded upon the content to provide more specificity relating to testing of application-based controls.

44. How should management address deficiencies and gaps in application controls?

There are two possible ways for management to address application control deficiencies. The first and most obvious approach is to perform a gap analysis of the process or control that is either designed or operating ineffectively, and develop an action plan to close the gap. The other possibility, which may be appropriate at least in the short term, is to make sure there is a thorough risk analysis of the deficiency, and also, of the surrounding compensating controls, if any, to determine the extent of the risk to relevant financial reporting assertions and whether the risk is adequately mitigated. This step may be vital in the short term because gap analysis and closure could require an extended period of time to complete, resulting in the correction of the IT control deficiency. In many cases, there is likely to be a significant increase in the need for manual detective controls that identify and correct specific items that could result in errors or omissions at the business process level. In situations involving high transaction volumes or highly complex transactions, this could present a significant and costly challenge.

45. How will the external auditor view application controls during the attestation process?

This obviously is a question that each external audit firm must address with its audit clients. It is safe to say, however, that the independent accountant will have IT-related risks and controls in mind when evaluating the basis for management's assertions in the internal control report. In late 2004, nine leading audit firms, including the Big 4, released "A Framework for Evaluating Control Exceptions and Deficiencies." This framework provides some insight into how the firms perceive the impact of IT general controls and application controls on financial reporting integrity. In general, the firms noted that "IT General Controls do not directly result in misstatements." Instead, they impact application controls, and "misstatements may result from ineffective application controls." A weakness in general IT controls potentially could have an effect on significant transactions and accounts through its impact on application controls. Therefore, a weakness in general IT controls could require remediation because its pervasive impact could unduly complicate management's assessment of internal control over financial reporting and the auditor's attestation of that assessment.

For example, we are aware of instances in which external audit firms are informing their audit clients that the company must develop stronger and more preventive controls over application security, in particular with respect to the administration of security roles and the security over access by users. For this reason, Section 404 compliance teams should assess the IT control environment, including the general IT and application controls, as early as possible in the process to determine whether there are gaps that must be addressed. Failure to do so could expose the company to difficulty with the attestation process.

Section 10: ERP Compliance Software and Automated Testing Tools

46. What are some examples of SOA enablement software to consider?

Vendors may be broken down into five categories:

- ERP compliance applications and document repositories: Emerging products include Oracle E-business Suite's Internal Control Manager (ICM), PeopleSoft's Internal Control Enforcer (ICE) and SAP's Management of Internal Controls (MIC).
- ERP compliance and testing solutions: Some of the companies providing products to the market include Applimation, Approva, Consul, CSI, D2C, LogicalApps, PCI, QSmart, Qsoftware and Virsa.
- Risk Management and Internal Audit Software: Examples include Paisley's Risk Navigator and AutoAudit, and Protiviti's Governance Portal.
- Document Management: Examples include Documentum and Stellent.
- Business Process Automation: Examples include Certus, HandySoft and OpenPages.

Many of the ERP systems have developed integrated compliance tools. In addition, numerous third-party software vendors have introduced other products into the market. In evaluating software solutions, organizations must consider specific business needs as well as functional requirements. For example, an organization utilizing multiple ERP systems will need software solutions that provide cross-platform capabilities. As with any software purchase, consideration must be given to specific hardware requirements. Also, management should be aware that existing infrastructure may play a role in the ultimate decision. For example, a fully implemented ERP may be used in the compliance solution. Likewise, if a particular vendor's document management solution is used, this system may provide a good leveraging point for additional governance functionality.

As noted throughout this publication, it is critical to realize that automated assessment tools are not "silver bullets." As with any software package, they typically require significant planning and setup efforts to ensure their effectiveness in each unique environment. When considering the purchase of one of these tools, organizations should consider the following:

- Allow enough time and resources to deal with initial results provided by the assessment tools. Many organizations feel overwhelmed by the resulting output of initial assessments performed by these tools. It is important to remember at the beginning that over time the root cause of exceptions and results must be analyzed to drive continuous improvement of the underlying processes and controls.
- Integrate the tool(s) into the ongoing process to ensure that the control environment improves over time. Tools used once a year to analyze environments often find similar results each year as the root-cause of the issues is never identified and resolved, and process improvements and preventive techniques are not implemented to eliminate the issues going forward.
- Ensure that the individuals implementing, configuring and utilizing the tools are knowledgeable of not only the tool being implemented, but also of the application that is being assessed, the business processes in scope and the related risks and controls.

47. What questions should be addressed with respect to evaluating an application's capability to support an SOA compliance effort?

While there are many questions to consider relating to testing capability, auditing capability, documentation repository, project facilitation and other matters, we have listed a few important ones below:

Will my system provide a sound repository for my compliance information?

Ensure that the system's information structures are flexible enough to allow the organization to access information in meaningful ways. These structures must provide a means of understanding control operating

effectiveness from different financial reporting perspectives. For example, the system should have robust risk and control linkages that support many-to-many relationships. A single control may address multiple financial reporting assertions. Controls existing in one area of the business may address risks existing in another area. In other words, control points may be upstream or downstream in the transaction flow from the source of the risk, as well as at the source of the risk. The system must accommodate this linkage of risks and controls.

In addition, the information structures upon which the system is based should allow for documentation at varying levels of the organizational and process hierarchy. One activity may need to go only two levels deep while another may require a third or fourth level of detail. As a result, the information structures should be able to support a multiple number of levels.

Will my system facilitate business owner involvement?

Over time, end users need to be involved in the compliance effort. For example, consider the four key points below:

1. The system must support workflow around key compliance activities (e.g., testing, documentation, evaluation and remediation).

2. The system should be underpinned by a self-assessment engine that supports continuous self-assessment around a variety of compliance activities, e.g., Section 302 certification, quarterly change reviews or Section 404 entity-level reviews. Other activities could include specific control assessments as well as non-SOA-related topics, such as violations of the code of ethics.

3. If self-assessment is used, the workflow relating to self-assessment must be enabled through a notification engine that alerts individuals to their assigned assessment responsibilities. Notification can be around the completion of tasks, resolution of action items, or exceptions that have occurred.

4. The system should provide central navigation points that support a simplified end-user experience.

Does the system support change control?

The information repository is a living history of an organization's control environment. Thus, tracking and management of change is essential. The system should support document versioning, provide audit trails for changes to risk and control information, and give users the ability to archive point-in-time evaluations. A sufficiently granular security structure to limit users to performing only their assigned roles within the assigned content areas also should be in place.

Does the system offer adequate reporting capabilities?

Reporting should ultimately present information that supports the overall assertions around financial reporting. That is where everything comes together. Summary and graphic reports with drill-down capabilities, as well as ad hoc clearing capability that supports extraction of all key data points available in the system, are needed. In addition, report-and-search mechanisms should provide flexible filtering criteria so that end users can pull specified data from the system. Finally, reporting also should employ security features that will make the tool one that business owners can utilize without fear of compromising system integrity.

Does the system support the way I intend to manage the compliance effort?

When choosing compliance software, consider whether the process will be managed in a centralized or a decentralized fashion. If decentralized, elements such as workflow and security will be very important. However, if centralized, the less important these factors become.

Also, be sure to understand how the tool will improve the compliance effort over time. For instance, how much of the data is configured or enabled on a "one time" basis, and how much must be redone as part of next year's compliance effort? Another example would be the ability to analyze the identified exceptions to distinguish the ones which have continued to exist over multiple reviews from new exceptions discovered for the first time.

Is the recommended software plug-and-play? Generally speaking, what are aspects of the software that I might need to configure and/or are able to be customized?

First and foremost, make sure the system is easily configurable by users, that is, it does not require extensive customization. Areas to be aware of that typically require a degree of flexibility in configuration are as follows:

- The levels of hierarchy supported (e.g., the necessary organizational and process hierarchies, which often vary by company)
- Drop-down selections (e.g., value lists)
- The content of self-assessment questions
- Workflow requirements
- In advanced scenarios, user-defined fields

A highly configurable system should be the goal. A system requiring too much customization is more expensive and challenging to maintain. However, an application should support customized reporting capabilities.

Will my auditor be able to rely on this tool and its results?

A key consideration of a compliance software tool also should be the various parties it is intended to support. When dealing with SOA compliance-related software, special thought should be given to the needs of the external auditors. If the auditor has a preferred software package or has already "certified" a certain package as one that they can rely on for their testing purposes, this may be a differentiator for overall cost savings after implementation. Be aware that if this tool becomes integral to managing user access within the ERP, it may be considered a key control itself and will need to be tested for SOA compliance.

48. How does the Section 404 compliance team differentiate between SOA-relevant controls in the ERP (which require documentation and testing) and the SOA compliance functionality?

These are separate concepts, but are often confused. There is a distinct difference between consideration of an application's controls (as discussed in Section 3) and consideration of the functionality of an application designed to support the SOA compliance process. Some of this confusion is due to the fact that many of the leading application providers today also offer SOA compliance solutions as part of their application functionality.

These SOA compliance solutions and tools do not execute controls. Instead, they facilitate the identification, documentation, and evaluation of the key controls which exist in business applications and processes. These are the controls which become the focal point of the compliance process. The compliance solution facilitates the workflow and reporting of results needed to conduct and complete the process. To optimize controls over time, organizations will seek to link the controls documented in their compliance repository to the points at which those controls are executed in their business processes. This could be in an ERP, an automated document repository, or through any variety of applications outside of an ERP.

Section 11: About Protiviti Inc.

Protiviti is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

Protiviti, which has more than 50 locations in North America, Latin America, Europe, Asia and Australia, is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Sarbanes-Oxley Services

Protiviti assists companies with Sarbanes-Oxley compliance efforts by helping them to document their internal control over financial reporting and disclosure controls and procedures, design and recommend improvements in processes and controls, and organize and manage projects for complying with the Sarbanes-Oxley Act.

Application Controls Effectiveness (ACE) Services

Protiviti's ACE solutions are designed to smartly tackle application risks when and where they are needed most. Our team includes professionals with years of application implementation, assessment and improvement experience who utilize our powerful methodologies and tools to help our clients effectively leverage their enterprise applications into holistic, integrated compliance and risk management solutions. Our services are relevant whether an organization is implementing a new application or trying to improve their management of a current installation. We help our clients:

- Manage Implementation Project Risk – align project delivery with internal control and compliance objectives for their application implementations or upgrades and provide an independent perspective through assessment, monitoring and reporting of project risks throughout the application project lifecycle.
- Optimize Automated Controls – evaluate and optimize the operating effectiveness of key application configurations and features used to support internal control and other compliance efforts, while reducing reliance on inefficient manual control techniques.
- Enhance Security and Segregation of Duties – evaluate and design effective user roles and segregation of duty (SoD) frameworks, security administration processes and global security parameters.
- Enable Compliance Automation Software – select, plan and integrate powerful software tools and supporting processes that improve internal control and compliance capabilities.
- Support Audit and Compliance Assessments – improve the quality and efficiency of application audits and assessments by utilizing specialized knowledge, experience and tools to manage the unique complexities of application control documentation and testing.

In addition, we have routine dialogue and active working arrangements with leading ERP vendors and related compliance software vendors, including Applimation, Approva, Oracle/PeopleSoft, SAP, Stellent and Virsa, as well as informal relationships with numerous other vendors. These alliance relationships enable our professionals to keep up-to-date with the latest product developments and to help our clients understand the unique benefits these varied solutions can provide.

North America

UNITED STATES
+1.888.556.7420
protiviti.com

CANADA
+1.416.350.2181
protiviti.ca

Europe

FRANCE
+33.1.42.96.22.77
protiviti.fr

GERMANY
+49.69.963768.100
protiviti.de

ITALY
+39.02.655.06.301
protiviti.it

THE NETHERLANDS
+31.20.346.04.00
protiviti.nl

UNITED KINGDOM
+44.207.930.8808
protiviti.co.uk

Latin America

MEXICO
+52.9171.1501
protiviti.com.mx

Asia-Pacific

AUSTRALIA
+61.3.9948.1200
protiviti.com.au

CHINA
+86.21.63915031
protiviti.cn

JAPAN
+81.3.5219.6600
protiviti.jp

SINGAPORE
+65.6220.6066
protiviti.com.sg

SOUTH KOREA
+82.2.2198.2065
protiviti.co.kr

Protiviti is a leading provider of independent risk consulting and internal audit services. The firm provides consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assists in the implementation of the processes and controls to enable their continued monitoring. Protiviti also offers a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti.com 1.888.556.7420